Nmap is a free open source tool, employed to discover hosts and services on a computer network by sending packets and analyzing the retrieved responses. Nmap offers some features for probing computer networks, including host discovery and service and operating system detection.

* Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses.
* Host discovery – Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.
* Port scanning – Enumerating the open ports on target hosts.
* OS detection – Determining the operating system and hardware characteristics of network devices.
* Version detection – Interrogating network services on remote devices to determine the application name and version number.
* Scriptable interaction with the target support using the Nmap Scripting Engine (NSE).

**Usage of Nmap**

* Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it.
* Identifying open ports on a target host in preparation for auditing.
* Network inventory, network mapping, and maintenance and asset management.
* Auditing the security of a network by identifying new servers.
* Generating traffic to hosts on a network, response analysis and response time measurement.
* Finding and exploiting vulnerabilities in a network.
* DNS queries and subdomain search

**NMAP Commands Cheatsheet**

The following section explains the usage of category-wise NMAP diverse commands with examples as following -

**Basic Scanning Commands**

| **Goal** | **Command** | **Example** |
| --- | --- | --- |
| Scan a Single Target | nmap [target] | nmap 192.168.0.1 |
| Scan Multiple Targets | nmap [target1, target2, etc | nmap 192.168.0.1 192.168.0.2 |
| Scan a Range of Hosts | nmap [range of ip addresses] | nmap 192.168.0.1-10 |
| Scan an Entire Subnet | nmap [ip address/cdir] | nmap 192.168.0.1/24 |
| Scan Random Hosts | nmap -iR [number] | nmap -iR 0 |
| Excluding Targets from a Scan | nmap [targets] – exclude [targets] | nmap 192.168.0.1/24 –exclude 192.168.0.100, 192.168.0.200 |
| Excluding Targets Using a List | nmap [targets] – excludefile [list.txt] | nmap 192.168.0.1/24 –excludefile notargets.txt |
| Perform an Aggressive Scan | nmap -A [target] | nmap -A 192.168.0.1 |
| Scan an IPv6 Target | nmap -6 [target] | nmap -6 1aff:3c21:47b1:0000:0000:0000:0000:2afe |

**Discovery Options**

| **Goal** | **Command** | **Example** |
| --- | --- | --- |
| Perform a Ping Only Scan | nmap -sP [target] | nmap -sP 192.168.0.1 |
| Don’t Ping | nmap -PN [target] | nmap -PN 192.168.0.1 |
| TCP SYN Ping | nmap -PS [target] | nmap -PS 192.168.0.1 |
| TCP ACK Ping | nmap -PA [target] | nmap -PA 192.168.0.1 |
| UDP Ping | nmap -PU [target] | nmap -PU 192.168.0.1 |
| SCTP INIT Ping | nmap -PY [target] | nmap -PY 192.168.0.1 |
| ICMP Echo Ping | nmap -PE [target] | nmap -PE 192.168.0.1 |
| ICMP Timestamp Ping | nmap -PP [target] | nmap -PP 192.168.0.1 |
| CMP Address Mask Ping | nmap -PM [target] | nmap -PM 192.168.0.1 |
| IP Protocol Ping | nmap -PO [target] | nmap -PO 192.168.0.1 |

| **ARP Ping** | **nmap -PR [target]** | **nmap -PR 192.168.0.1** |
| --- | --- | --- |
| Traceroute | nmap –traceroute [target] | nmap –traceroute 192.168.0.1 |
| Force Reverse DNS Resolution | nmap -R [target] | nmap -R 192.168.0.1 |
| Disable Reverse DNS Resolution | nmap -n [target] | nmap -n 192.168.0.1 |
| Alternative DNS Lookup | nmap –system-dns [target] | nmap –system-dns 192.168.0.1 |
| Manually Specify DNS Server(s) | nmap –dns-servers [servers] [target] | nmap –dns-servers 201.56.212.54 192.168.0.1 |
| Create a Host List | nmap -sL [targets] | nmap -sL 192.168.0.1/24 |

**Advanced Scanning Options**

| **Goal** | **Command** | **Example** |
| --- | --- | --- |
| TCP SYN Scan | nmap -sS [target] | nmap -sS 192.168.0.1 |
| TCP Connect Scan | nmap -sT [target] | nmap -sT 192.168.0.1 |
| UDP Scan | nmap -sU [target] | nmap -sU 192.168.0.1 |
| TCP NULL Scan | nmap -sN [target] | nmap -sN 192.168.0.1 |
| TCP FIN Scan | nmap -sF [target] | nmap -sF 192.168.0.1 |
| Xmas Scan | nmap -sX [target] | nmap -sX 192.168.0.1 |
| TCP ACK Scan | nmap -sA [target] | nmap -sA 192.168.0.1 |
| Custom TCP Scan | nmap –scanflags [flags] [target] | nmap –scanflags SYNFIN 192.168.0.1 |
| IP Protocol Scan | nmap -sO [target] | nmap -sO 192.168.0.1 |
| Send Raw Ethernet Packets | nmap –send-eth [target] | nmap –send-eth 192.168.0.1 |
| Send IP Packets | nmap –send-ip [target] | nmap –send-ip 192.168.0.1 |

**Port Scanning Options**

| **Goal** | **Command** | **Example** |
| --- | --- | --- |
| Perform a Fast Scan | nmap -F [target] | nmap -F 192.168.0.1 |
| Scan Specific Ports | nmap -p [port(s)] [target] | nmap -p 21-25,80,139,8080 192.168.1.1 |
| Scan Ports by Name | nmap -p [port name(s)] [target] | nmap -p ftp,http\* 192.168.0.1 |
| Scan Ports by Protocol | nmap -sU -sT -p U: [ports],T:[ports] [target] | nmap -sU -sT -p U:53,111,137,T:21- 25,80,139,8080 192.168.0.1 |
| Scan All Ports | nmap -p ‘\*’ [target] | nmap -p ‘\*’ 192.168.0.1 |
| Scan Top Ports | nmap –top-ports [number] [target] | nmap –top-ports 10 192.168.0.1 |
| Perform a Sequential Port Scan | nmap -r [target] | nmap -r 192.168.0.1 |

**Version Detection**

| **Goal** | **Command** | **Example** |
| --- | --- | --- |
| Operating System Detection | nmap -O [target] | nmap -O 192.168.0.1 |
| Submit TCP/IP Fingerprints | [www.nmap.org/submit/](https://nmap.org/submit/) |  |
| Fingerprints |  |  |
| Attempt to Guess an Unknown OS | nmap -O –osscan guess [target] | nmap -O –osscan-guess 192.168.0.1 |
| Service Version Detection | nmap -sV [target] | nmap -sV 192.168.0.1 |
| Troubleshooting Version Scans | nmap -sV –version trace [target] | nmap -sV –version-trace 192.168.0.1 |
| Perform a RPC Scan | nmap -sR [target] | nmap -sR 192.168.0.1 |

**Firewall Evasion Techniques**

| **Goal** | **Command** | **Example** |
| --- | --- | --- |
| augment Packets | nmap -f [target] | nmap -f 192.168.0.1 |
| pacify a Specific MTU | nmap –mtu [MTU] [target] | nmap –mtu 32 192.168.0. |
| Use a Decoy | nmap -D RND:[number] [target] | nmap -D RND:10 192.168.0.1 |
| le Zombie Scan | nmap -sI [zombie] [target] | nmap -sI 192.168.0.38 |
| Manually Specify a Source Port | nmap –source-port [port] [target] | nmap –source-port 10 192.168.0.1 |
| Append Random Data | nmap –data-length [size] [target] | nmap –data-length 2 192.168.0.1 |
| Randomize Target Scan Order | nmap –randomize-hosts [target] | nmap –randomize-ho 192.168.0.1-20 |
| Spoof MAC Address | nmap –spoof-mac [MAC|0|vendor] [target] | nmap –spoof-mac Cis 192.168.0.1 |
| Send Bad Checksums | nmap –badsum [target] | nmap –badsum 192.168.0.1 |

**Troubleshooting And Debugging**

| **Goal** | **Command** | **Example** |
| --- | --- | --- |
| Getting Help | nmap -h | nmap -h |
| Display Nmap Version | nmap -V | nmap -V |
| Verbose Output | nmap -v [target] | nmap -v 192.168.0.1 |
| Debugging | nmap -d [target] | nmap -d 192.168.0.1 |
| Display Port State Reason | nmap –reason [target] | nmap –reason 192.168.0.1 |
| Only Display Open Ports | nmap –open [target] | nmap –open 192.168.0.1 |
| Trace Packets | nmap –packet-trace [target] | nmap –packet-trace 192.168.0.1 |
| Display Host Networking | nmap –iflist | nmap –iflist |
| Specify a Network Interface | nmap -e [interface] [target] | nmap -e eth0 192.168.0.1 |

**NMAP Scripting Engine**

| **Goal** | **Command** | **Example** |
| --- | --- | --- |
| Execute Individual Scripts | nmap –script [script.nse] [target] | nmap –script banner.nse 192.168.0.1 |
| Execute Multiple Scripts | nmap –script [expression] [target] | nmap –script ‘http-\*’ 192.168.0.1 |
| Script Categories | all, auth, default, discovery, external, intrusive, malware, safe, vuln |  |
| Execute Scripts by Category | nmap –script [category] [target] | nmap –script ‘not intrusive’ 192.168.0.1 |
| Execute Multiple Script Categories | nmap –script [category1,category2,etc] | nmap –script ‘default or safe’ 192.168.0.1 |
| Troubleshoot Scripts | nmap –script [script] –script trace [target] | nmap –script banner.nse –script-trace 192.168.0.1 |
| Update the Script Database | nmap –script-updatedb | nmap –script-updatedb |